

Patent claims

1. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that
 - the operation (h) is disguised before its execution,
 - the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$), and
 - the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1}) with disguised input data ($x \otimes R_1$) yields output data (y) identical with the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x).
2. A data carrier according to claim 1, characterized in that at least one random number (R_1) enters into the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$).
- SUB 17 3. A data carrier according to either of the above claims, characterized in that the determination of the disguised operation (h_{R1}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.
4. A data carrier according to any of the above claims, characterized in that the disguised operation (h_{R1}) is permanently stored in the data carrier in advance.
5. A data carrier according to claim 4, characterized in that at least two disguised operations ($h_{R1}, h_{R1'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations ($h_{R1}, h_{R1'}$) is selected randomly when a disguised operation is to be executed.
- SUB 27 6. A data carrier according to any of claims 1 to 3, characterized in that the disguised operation (h_{R1}) is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation.

SUBA27 7. A data carrier according to any of the above claims, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

8. A data carrier according to claim 7, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1).

9. A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that

- the operation (h) is disguised before its execution,
- the disguised operation (h_{R1}) is executed with disguised input data ($x \otimes R_1$),
- the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1R2}) with disguised input data ($x \otimes R_1$) yields output data ($y \otimes R_2$) which are disguised relative to the output data (y) determined upon execution of the undisguised operation (h) with undisguised input data (x), and
- the undisguised output data (y) can be determined from the disguised output data ($y \otimes R_2$) with the aid of data (R_2) used for disguising the operation (h).

10. A data carrier according to claim 9, characterized in that at least one random number (R_1) enters into the determination of the disguised input data ($x \otimes R_1$) and at least two random numbers (R_1, R_2) enter into the determination of the disguised operations (h_{R1R2}).

SUBA37 11. A data carrier according to either of claims 9 and 10, characterized in that the determination of the disguised operation (h_{R1R2}) and the disguised input data ($x \otimes R_1$) is effected with the aid of EXOR operations.

12. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation (h_{R1R2}) is permanently stored in the data carrier in advance.

13. A data carrier according to claim 12, characterized in that at least two disguised operations ($h_{R_1R_2}$, $h_{R_1'R_2'}$) are permanently stored in the data carrier in advance and one of the stored disguised operations ($h_{R_1R_2}$, $h_{R_1'R_2'}$) is selected randomly when a disguised operation is to be executed.
14. A data carrier according to claim 13, characterized in that the random numbers (R_1 , R_2) for determining the first disguised operation ($h_{R_1R_2}$) are inverse to the random numbers (R_1' , R_2') for determining the second disguised operation ($h_{R_1'R_2'}$) with respect to the combination used for determining the disguised operations ($h_{R_1R_2}$, $h_{R_1'R_2'}$).

SUB A47 15. A data carrier according to any of claims 9 to 11, characterized in that the disguised operation ($h_{R_1R_2}$) is recalculated before its execution and the random numbers (R_1 , R_2) are redetermined for said calculation.

16. A data carrier according to any of claims 9 to 15, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

17. A data carrier according to claim 16, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data (y) contained in the table is effected by combination with the at least one further random number (R_2).

SUB A57 18. A data carrier according to any of the above claims, characterized in that the operation (h) is a nonlinear operation with respect to the combination used for disguising the operation (h).